UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. HAOYANG YU, *et al.* Defendants	CRIMINAL No. 1:19-cr-10195-WGY

GOVERNMENT'S TRIAL MEMORANDUM

The United States respectfully submits this summary of the evidence it expects to present in its case-in-chief at the trial of defendant Haoyang Yu. This overview seeks to highlight the principal aspects of the upcoming trial and to alert the Court to potential evidentiary and other issues. It is not an exhaustive recitation of the evidence the government intends to offer.

I. CASE SUMMARY AND INDICTMENT

At the heart of this case are allegations that the defendant possessed and stole trade secrets relating to the design and development of microchips known as monolithic microwave integrated circuits (MMICs).[1] The Second Superseding Indictment (SSI) further alleges that those trade secrets rightfully belonged to the defendant's now-former employer, Analog Devices, Inc. (ADI), a global leader in the design and manufacturing of integrated circuits.[2] The rest of the alleged

[1] The technology at issue here is state-of-the-art, performing functions such as power amplification, low-noise amplification, and high-frequency switching. MMICs are used in radio, cellular, and satellite communications and in defense and aerospace applications.

[2] The SSI charges the defendant with Theft of Trade Secrets, in violation of 18 U.S.C. § 1832(a)(1), (a)(2), and (a)(4); Possession of Trade Secrets, in violation of 18 U.S.C. § 1832(a)(3) and (a)(4); Wire Fraud, in violation of 18 U.S.C. § 1343; Illegal Exports of Controlled Technology, in violation of 18 U.S.C. § 1705; Visa Fraud, in violation of 18 U.S.C. § 1546; and Unlawful Procurement of Citizenship or Naturalization, in violation of 18 U.S.C § 1425(a).

criminal conduct flows from the defendant's trade secret theft. For example, the SSI also alleges that the defendant committed wire fraud by falsely claiming rightful ownership of the technology he sent to a Taiwanese MMICs manufacturer; violated export laws by transmitting said technology to Taiwan without the requisite export licenses; and committed immigration and naturalization fraud by concealing his criminal conduct from authorities.

A. Background

The defendant began work as an ADI MMIC designer in July 2014, just a few days after he was hired into the same position at Hittite Microwave Corporation (Hittite), a company that ADI then acquired. Both ADI and Hittite required Yu to sign confidentiality agreements in which he promised not to make use of or to disclose confidential information. At both at ADI and Hittite, Yu also agreed to refrain from engaging in outside employment that would conflict with obligations to his employer.

Nonetheless, while ADI employed him, Yu and his co-defendant wife established Tricon MMIC, LLC (Tricon), a business specializing in wideband MMIC amplifiers and providing integrated circuit design to customers in the defense, aerospace, and satellite industries. Yu quit ADI on July 31, 2017. Before he left, a supervisor warned him not to remove ADI's proprietary information; he acknowledged the warning. On his final day, Yu also signed a Proprietary Rights Statement acknowledging his legal obligation to maintain the confidentiality of ADI's proprietary information, including, among other things, all technical material – including schematics and layouts – relating to present and future product designs and all customer information, including the volumes and products those customers ordered. Agents later found Yu's signed copy of this statement in his home office, from which he built an illegal business based precisely on the proprietary trade secret information he had promised to honor.

B. Trade Secrets Charges (Counts 1-11)

1. Yu Stole ADI's Confidential Files.

During Yu's last ten months at ADI, he systematically accessed thousands of confidential files on ADI's secure network. Yu downloaded these files to his ADI laptop computer and then uploaded the data to his account with Google Drive, a cloud storage service. Available records don't identify the names of the files that the defendant uploaded, but court-ordered searches of the Google Drive account and of the defendant's personal computers later uncovered thousands of stolen ADI files. The clearest evidence of this theft is that these thousands of ADI trade secret files not only contained information essential to MMIC design but also bore the same hash values as files on the ADI servers. A hash value is an alphanumeric code that uniquely identifies the data in a computer file. If that data is modified even by a single character, the hash value will change dramatically. Thus, any two files with identical hash values also contain identical information. In this case, thousands of files on the defendant's computers have hash values that match files on ADI's servers. This means that the files are identical and, therefore, must have a common source: ADI.

Ample evidence demonstrates the defendant's intent to purloin confidential files and to conceal his activity from ADI. As just one example, when downloading some of ADI's most valuable secrets to his work laptop, the defendant purposefully renamed the files with innocuous names designed to conceal their contents.[3] In some cases, the defendant used the names of characters from a children's fantasy game. In another case, he gave a moniker – "kids8600.jpg" – apparently designed to camouflage the file as a picture of children. ADI had named this file

[3] Changing the name of a file does not change the content of the file and, thus, does not change its hash value.

"K8600_TOP.gds." It contains blueprints for 11 ADI microchips. Anyone in possession of this file has all of the information needed to commission the manufacture of those MMICs.

2. ADI Took Extensive Measures to Keep Confidential Information Secret.

In addition to requiring a confidentiality agreement and reminding Yu of his confidentiality obligations when the defendant left the company, ADI took numerous steps to safeguard its trade secrets.[4] Specifically, ADI issued employee badges to enforce restrictions on physical access to company facilities. It required user accounts and strong passwords in order to restrict access to computer networks. The company used network security mechanisms, such as encryption and firewalls, to control the devices that could connect to the ADI network. The information stored on ADI's networks was compartmentalized, and ADI prevented employees from accessing portions of the network that did not pertain to their work. Thus, highly confidential trade secrets, such as MMIC design files, were not generally accessible to all ADI employees. In addition, whenever ADI presented such confidential information internally, the presentations included warnings that the information was proprietary and confidential. When information about ADI devices was shared outside the company, recipients were required to sign non-disclosure agreements, and the information was marked as proprietary and confidential.

3. ADI's Trade Secrets Derive Value from Being Neither Generally Known Nor Readily Ascertainable.

The trade secrets the defendant stole fall into two categories: (1) secrets related to ADI's MMIC designs and design processes; and (2) customer and financial information.

[4] To prove information is a trade secret, the government must prove that (1) the owner took reasonable measures to keep such information secret and that (2) the information derives independent economic value from not being generally known to, and not being readily ascertainable by, another person who can obtain economic value from disclosure of the information. 18 U.S.C. § 1839(3).

a. MMIC Designs and Design Processes

The design-related trade secrets[5] Yu stole are best understood in the context of the steps – from conception through production – required for ADI to design and build a MMIC that a customer can buy. That process is depicted graphically below.

Development begins by determining the MMIC's performance requirements, *i.e.* what the target customers would like the chip to do. ADI then generates a conceptual design, a rough sketch of the MMIC architecture. This starting point relies on ADI's knowledge of design, production, and manufacturing. The quality of the conceptual design is important because it informs subsequent design decisions and the efficiency of the overall development process.

With the conceptual design in hand, ADI selects the foundry that will manufacture the MMIC. It also chooses among the foundry's fabrication processes. In a crude way, these decisions can be likened to an architect choosing a construction crew (the foundry) and then choosing whether to make his structure out of wood, steel, or concrete (the fabrication process). Because wood, steel, and concrete have different properties and capabilities, the architect's choice will affect his plans for the structure. Similarly, the choice of foundry and fabrication process affects how ADI designs its chip.

Based on his choice of foundry and process, a chip designer then selects what is called a process design kit (PDK). A PDK is a library of files that model and describe the technical and physical parameters of a chip's basic building blocks – such as the transistors, transmission lines,

[5] A trade secret need only possess minimal novelty. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974). To determine whether the information derives independent economic value from being kept secret, courts most often consider "the degree to which the secret information confers a competitive advantage on its owner." *United States v. Chung*, 659 F.3d 815, 824–26 (9th Cir. 2011) (citing cases). This is "a fact-intensive inquiry" and may include considering the cost and effort necessary to develop the secret information. *Id.*

capacitors, and inductors. Foundries create these libraries so that engineers will be able to marry their conceptual design with physical plans that are, in turn, compatible with the fabrication process and an operational chip. In essence, these libraries give the engineers (architects) important information that must be accounted for in their design (blueprints) so that the resulting microchip (structure) will operate as expected. A foundry will provide a PDK that is specific to the selected manufacturing process, and an engineer can exclusively rely on this. However, ADI has invested in and developed its own proprietary modeling files that work in concert with a PDK issued by the foundry. These ADI modeling files capture additional chip properties and responses that are important to ADI's specific design needs, *i.e.*, the need to design a wideband MMIC that pushes the limits of the technology and, in so doing, provides a competitive advantage.

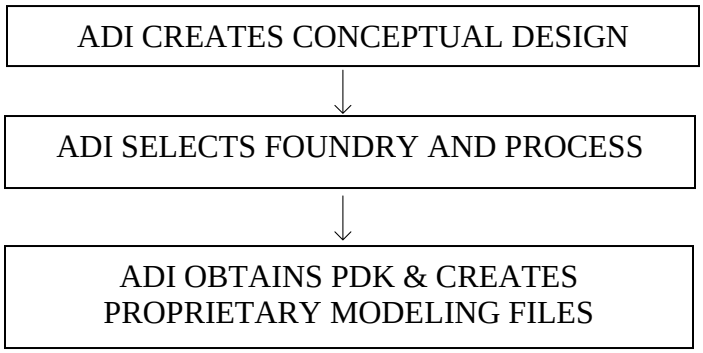
Focused design for the specific MMIC then begins. Engineers create a schematic, a formal rendering of the conceptual design. In conjunction with design software, the PDK, and ADI's proprietary modeling files, they use this schematic to simulate how the circuit will perform when the building blocks are assembled. Afterward, the schematic is translated into a physical representation. This is referred to as "design layout." As part of the layout process, ADI uses physics-based electromagnetic modeling to ascertain how the wires within the circuit interact with one another.[6] These results are fed back into the schematic simulation. This iterative loop – through circuit simulation, layout, and electromagnetic testing – is typically the most time-consuming part of the design process. The end result is ADI's confidence that a particular design will generate a microchip that meets the intended performance requirements.

[6] At higher frequencies, these interactions are extremely complicated, are difficult to predict, and greatly affect the performance of the circuit.

After ADI is satisfied with the simulated circuit performance, it converts the layout into a manufacturing file. The industry-standard format is a graphic design system, or GDS, file. A GDS file is akin to an architect's blueprint from which a construction crew (the foundry) can build the home (microchip). ADI electronically submits the GDS file to the foundry and requests a "tapeout" – *i.e.* that the foundry construct the microchip. The foundry uses the GDS file to build the multi-layered microchip and then sends the completed prototype to ADI.

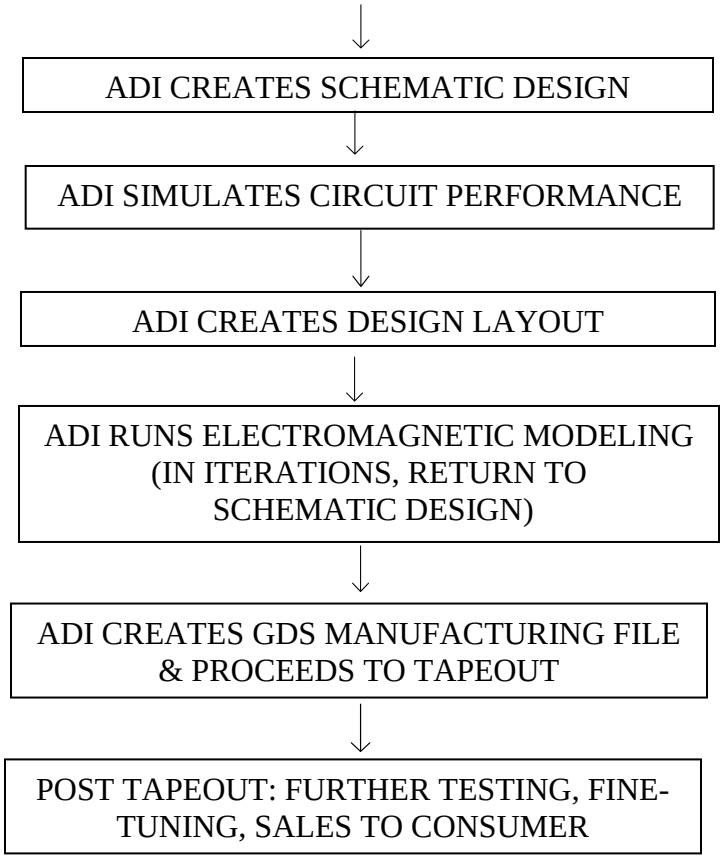
ADI tests the prototype to determine whether it performs in accordance with design goals and is sufficiently reliable and robust.[7] Upon reviewing those results, ADI typically performs additional iterations of the design and fabrication process to address shortcomings and improve performance. After ADI has verified the MMIC's performance, reliability, and robustness, the company is prepared to sell the MMIC. Partly because of the iterative nature of each of these processes, ADI invested hundreds of hours and millions of dollars in perfecting the files the defendant stole.[8]

ADI MMIC DEVELOPMENT FLOW



[7] Robustness is a MMIC's ability to perform to a high degree of reliability in the presence of harsh environmental conditions, such as extreme heat and cold. Robustness also measures the error rate at which the foundry will fabricate malfunctioning copies of the given MMIC and prioritizes a low error rate.

[8] Moreover, those stolen files themselves were, in many instances, refinements of intellectual property ADI acquired when it bought Hittite for $2 billion. The price ADI paid for Hittite is an indication of the value of the trade secrets in this case.



ADI creates and takes extensive measures to keep secret its intellectual property at each step of the design process depicted above. The trade secrets in this case are the specific tools ADI created – schematics, layout files, modeling files, manufacturing files – to design and build wideband MMICs that push the limits of the technology. The creation of each of these tools represents an investment of hundreds or thousands of hours of labor, thousands or millions of dollars, and the utilization of expertise that ADI has been cultivating for decades. The result of this investment of time, expense, and expertise is a product that is more precise, robust, and reliable than it would be absent such investment. These qualities confer on ADI a competitive advantage and, as evidence will demonstrate, are what motivates ADI's customers to choose the company.

With this MMIC development flow in mind, a simple example of the defendant's conduct with respect to a specific ADI part – HMC994A – demonstrates that he stole trade secrets with the intent of economically benefiting himself and with the knowledge that his actions would harm ADI, thus violating 18 U.S.C § 1832. The example: evidence will show that Yu stole numerous files relating to HMC994A. Yu was not involved in the design of that part, and therefore, *even while he was working at ADI*, Yu had no legitimate reason to access or possess files relating to it. Yu effected the theft in the manner described above. *See* section I.B.1., *supra*. That is, in October 2016, he (1) downloaded HMC994A design files, among others, from ADI's design data repository to his ADI laptop; (2) renamed one of the most valuable files kids8600.jpg; (3) ultimately moved kids8600.jpg to his personal computer; and (4) was later found to be in possession, on his personal computer, of a file with precisely the same hash value as the one he downloaded and renamed kids8600.jpg.

ADI released part HMC994A in April 2017, after – in many previous months – it had invested between $500,000 and $1,000,000 in labor and material.[9] Six weeks later, the defendant, still employed at ADI, sent the Taiwanese foundry a GDS file for a part substantially identical to HMC994A. Yu instructed the foundry to treat the GDS information "as proprietary data" and to use it to manufacture an analogous Tricon part named the TM5054. The criminal similarity of these two parts – the HMC994A and the TM5054 – will be demonstrated by expert testimony that geometric features on the two microchips match down to the minimum file resolution of one nanometer.[10] That testimony will include an opinion that the only plausible explanation for this

[9] ADI acquired an earlier version of this part in its acquisition of Hittite, but nonetheless expended the resources described here refining the product before releasing it in April 2017.

[10] A nanometer is 1/1,000,000,000 of a meter. The size of a single water molecule is about 1.5 nanometers. A strand of hair is about 80,000 to 100,000 nanometers wide

precision is that the GDS files share a common source. Indeed, the defendant advertised the Tricon part as equivalent to HMC994. Yu later marketed this product widely, including offering it to ADI's customers.[11]

b. Customer and Financial Data

Similar proof will establish that Yu stole – *i.e*. downloaded from ADI's network and later moved to his personal computer – sensitive customer data. For example, he stole sales data that showed precisely which microchips individual customers had purchased, how many they bought, and how much they paid. There was no business reason for Yu, a MMIC designer, to possess this information on his personal computer or even to have downloaded it to his company laptop. However, Yu's motivation is clear: customer and financial data allowed Yu to set his pricing strategy at Tricon and to target specific ADI customers. ADI takes reasonable measures to protect its customer and financial information by limiting access to it, providing confidentiality training to employees, designating the information confidential, and requiring confidentiality agreements whenever it is shared. The secrecy of this data confers on ADI a competitive advantage because, in order to achieve an adequate rate of return on products that are extraordinarily expensive to design and often sold in low quantities, ADI must command adequate margins. Armed with this secret information, a competitor – especially one who stole the designs – can unfairly undercut ADI's prices.

C. <u>Wire Fraud Charges</u> (Counts 12-14)

Win Semiconductor Corp. (Win) is a MMIC foundry located in Taiwan. Both ADI and Tricon hired this manufacturer to fabricate their products. Yu initiated his relationship with Win

[11] The defendant marketed and sold numerous MMICs that are virtually identical to ADI products. Tricon also targeted ADI customers by advertising its parts as substitutes for ADI's.

in early 2017, when he submitted paperwork to establish a Win account. In those documents, he described Tricon as a small company whose innovations, flexibility, and lack of overhead allowed it to offer competitive prices.[12] He added, "Our IP gives us a leg up against our competitors in terms of some key parameters for microwave amplifiers." Ultimately, Tricon and Win executed mutual agreements not to disclose the other's proprietary information. Without these agreements and the assurance that Tricon, in fact, owned the intellectual property it was transmitting for MMIC production, Win would not have produced Tricon MMICs. Thus, the defendant concealed from Win a material fact – namely, that the MMIC designs he sent were stolen from ADI. Over the next two years, Yu and his co-defendant, Chen, followed this deceit with four international wire payments for Win's services.

D. Export Charges (Counts 15-16)

The defendant commissioned Win to manufacture 16 separate microchips and electronically transmitted the GDS files for each of those chips to Win in Taiwan. The Export Administration Regulations (EAR) control the export of "dual-use items," that is, commercial items that also have a military application, to foreign countries. The EAR control the export of both goods and technology, such as the GDS files Yu sent to Win. As relevant to the export charges, the EAR classify two of those files – those for microchips TM5051 and TM5052 – as requiring a license for export to Taiwan, for national security and anti-terrorism reasons. The evidence will show the defendant knew of this licensing requirement yet exported the technology without obtaining a license.

//

[12] In dealings with Win and with Tricon customers, the defendant used the pseudonym Jack Yu. He also used the pseudonym Jack Tricon.

E. Immigration Charges (Counts 17-18)

Digital forensics show that Yu began copying ADI trade secrets no later than September 2016. Therefore, the defendant had already repeatedly committed trade secret crimes by February 15, 2017, when he was interviewed by a U.S. Citizenship and Immigration Services adjudication officer. There, in connection with his Application for Naturalization, Yu affirmed – among other false statements – that he had not "ever committed… a crime or offense for which … [he] was not arrested." The evidence will show that Yu deliberately made this false statement in order to obtain U.S. citizenship and that, if he had truthfully disclosed his looting of ADI's trade secrets, he would likely have been legally disqualified from consideration.

F. Proof Relevant to Application of the U.S. Sentencing Guidelines

In addition to evidence proving the elements of the charged crimes, the government will offer evidence to prove the following specific offense characteristics and upward adjustment.

1. Loss Amount - U.S.S.G. § 2B1.1(b)(1)

The Guidelines set forth a general rule that loss is the greater of actual loss or intended loss. U.S.S.G. § 2B1.1 n.3.A. Here, the government will offer evidence of both. Intended loss means the "pecuniary harm that the defendant purposefully sought to inflict," *id*. at n.3(A)(ii), which includes harm he would have inflicted "if the defendant had not been caught." *United States v. Frisch*, 704 F.3d 541 (8th Cir. 2013). To prove the scope of the defendant's intended harm, the government will offer – among other evidence – information on the scale of the defendant's theft of numerous trade secrets, including but not limited to those specified in the SSI; evidence of the million-dollar value of the MMIC inventory Yu had already manufactured; and his statements about future plans for the enterprise. The government will also offer evidence of what it cost ADI to develop the stolen information. *See* U.S.S.G. § 2B1.1 at n.3(C)(ii)

(including as a factor in estimating loss "[i]n the case of . . . trade secrets . . . the cost of developing that information or the reduction in value of that information that resulted from the offense.").

2. Transmitting a Trade Secret Out of the U.S. or to Benefit a Foreign Government or Instrumentality - U.S.S.G. § 2B1.1(b)(14)

This Guideline calls for an increase in the offense level by the greater of (A) two levels if the offense involved misappropriation of a trade secret and the defendant knew or intended that the trade secret would be transmitted out of the United States; or (B) four levels if the defendant knew or intended that the offense would benefit a foreign government, instrumentality, or agent. Both subsections apply here. The defendant's transmission of stolen GDS files to the Taiwanese foundry satisfies the former. The latter is satisfied because Yu sold his stolen MMICs to a company that he knew was part of the Turkish military and that he knew would use his stolen chips in their electronic warfare products. *See* SSI ¶ ¶ 14-15.

3. Special Skill Adjustment - U.S.S.G. § 3B1.3

This Guideline calls for a two-level upward adjustment if the defendant used a special skill in a manner that significantly facilitated the commission or concealment of the offense. A special skill is one "not possessed by members of the general public and usually requiring substantial education, training, or licensing." *See* U.S.S.G. § 3B1.3 at n.4. Here, the government will introduce evidence that the defendant concealed his crime by, among other things, removing ADI's markings from the manufacturing plans for Tricon's chips. This was obvious use of his advanced engineering skills to prevent detection of his crimes.

II. EVIDENCE AND ANTICIPATED EVIDENTIARY ISSUES

In the following section, the government summarizes witnesses and exhibits it will present at trial. In addition, the government highlights evidentiary issues that may arise. The government

views these issues as uncontroversial and will seek agreement as to admissibility. If, upon consultation with the defense, issues remain in dispute, the government will move *in limine* for rulings on admissibility.

A. Categories of Witnesses

1. ADI employees who will testify about:
   a) ADI policies
   b) ADI and Hittite personnel and human resources documents
   c) ADI security measures used to protect trade secrets
   d) The defendant's tenure at ADI
   e) The contents of Yu's Digital Guardian records
   f) ADI microchips and the process of their design
   g) Public release dates of various ADI parts
   h) ADI trade secrets, including proprietary digital information
   i) The process of identifying the hash values on ADI files
   j) The content of files identified as hash-value matches
   k) The types of files that ADI never makes public
   l) Computer comparisons of ADI and Tricon parts and files
   m) The specifications and performance data of ADI parts
   n) ADI business practices, models, marketing, and revenue
   o) The costs of developing ADI microchips

2. A representative from SAI Global, which administers and tracks ADI's employee training

3. Law enforcements witnesses regarding records and items seized from the defendant's residence; surveillance of the defendant; packages shipped by the defendant and intercepted by law enforcement; admissions by the defendant; records and computer files located on the defendant's electronic devices and in his electronic accounts

4. An FBI forensic examiner regarding the preservation, extraction, and forensic analysis of information obtained from searches of various electronic storage media; metadata, including dates when the information was created, saved, downloaded, and modified; and a comparison of files found in the defendant's electronic devices with files maintained on ADI computer servers. The latter will involve a summary of defendant files whose hash values are identical to those located on ADI's servers

5. An employee of I. Miller Precision Optical Instruments, Inc.

6. An FBI linguist who will testify about the translation of Chinese-language documents and records

7. A former FBI financial analyst, who will describe information contained in Tricon's bank records

8. Tricon customers

9. ADI customers

10. Win employees

11. A Department of Commerce witness regarding absence of licenses to export the MMIC technology specified in Counts 15 and 16

12. An official of the Department of Homeland Security, U.S. Citizenship and Immigration Services regarding the naturalization process and the materiality of the false statements by the defendant specified in Counts 17 and 18

13. Expert witnesses previously disclosed to the defense:

    a) A senior staff member in the Compound Semiconductor Optoelectronics Department at the Microsystems Science, Technology & Component Center at Sandia National Laboratories in Albuquerque, New Mexico regarding: (1) the nature of electromagnetic radiation and microwaves; the concept of amplification and applications for power amplifiers, such as the ones at issue here; the design and fabrication process for microchips; (2) the similarities between several ADI MMIC designs and their Tricon counterparts, including those listed in paragraph 9 of the SSI, and his opinion that that files used to produce the MMICs share are common source; (3) files for the MMICs specified in Counts 15 and 16 of the SSI would have produced microchips that performed as their specification and data sheets advertised; and (4) if necessary, the degree of effort, expense, and expertise required to reverse engineer ADI's GDS files to the level of accuracy and detail needed to produce comparable parts. This analysis will include the relative effort, expertise, and expense required to develop such a chip from scratch with that required to reverse engineer it from a photograph and, separately, to manufacture it from an existing GDS file. The witness may also opine about the content of these GDS and other relevant files gives them economic value.

    b) Official of the Department of Commerce, Bureau of Industry and Security regarding export control regime and the agency's determination that the technology specified in Counts 15 and 16 required a license for export to Taiwan

c) A former Foreign Area Officer at the Department of Defense who also served as a technical expert at the Department of State with responsibility for various aspects of U.S – Turkey relations, to testify about the Turkish company alluded to in paragraph 14 of the Second Superseding Indictment and its relationship to the Turkish government.

14. Keepers of Records
   a) Bank of America
   b) Federal Express
   c) Google
   d) Namecheap
   e) United Parcel Services
   f) Weebly

B. <u>Categories of Exhibits</u>

1. Tricon incorporation documents
2. Tricon marketing literature, including the contents of its website
3. Specification sheets and performance data for ADI and Tricon parts
4. Information stored on the defendant's electronic devices
5. Information stored in the defendant's electronic accounts
6. English translations of Chinese-language messages, business cards
7. The defendant's recorded statement and accompanying transcript
8. Physical evidence seized from the defendant's home
9. Photographs taken by surveillance teams
10. Photographs of physical evidence, including microchips
11. The defendant's personnel paperwork
12. Information on ADI and Hittite trainings and policies
13. Demonstrative exhibits describing MMICs, their function, their production
14. Digital Guardian records documenting the defendant's interactions with ADI network files
15. Summary exhibits of Digital Guardian data
16. Demonstrative exhibits describing electronic hash values and their significance
17. Exhibits listing thousands of ADI trade secret files found in the defendant's possession
18. Summary exhibits of thousands of ADI trade secret files found in the defendant's possession
19. Individual trade secret files – including but not limited to schematics, modeling files, layout files, manufacturing files, and customer data files – found in the defendant's possession
20. Electronic comparisons of ADI and Tricon chips and files

21. Exhibits illustrating expert analysis and conclusions about Tricon's microchips, including that Tricon's designs were similar to ADI's parts, were capable of producing certain electronic characteristics, and could not be readily ascertained through proper means
22. Demonstrative exhibits describing the development ADI parts
23. Summary exhibits describing the release dates of ADI parts
24. Win records describing its work with Tricon and the defendant
25. License determinations from the U.S. Department of Commerce
26. Documents showing that the defendant did not apply for export licenses
27. Tricon customer documents
28. ADI customer documents
29. ADI customer and financial data
30. Bank of America records
31. Summary exhibits describing Tricon revenues
32. Summary charts: ADI investment in and revenue from various parts
33. Documents from the defendant's immigration A-file
34. UPS paperwork
35. FedEx paperwork

C. Evidentiary Issues

1. Admissibility of Expert Testimony- Fed. R. Evid. 702

The jury in this case will be required to understand a number of subjects beyond the ken of the average juror. These include the nature of and process for developing the technology at issue and the regulatory regime that requires an export license for that technology. The touchstone for expert testimony is whether it is helpful to the jury's understanding of the evidence. In this case, the government's proffered expert testimony will not only be helpful to the jury's understanding; the absence of such testimony would likely result in confusion and an inability by the jury to understand the technical aspects or relevance of much of the evidence introduced at trial. The government is mindful of that such testimony "must be carefully circumscribed to assure that the expert does not usurp either the role of the trial judge in instructing the jury as to the applicable law or the role of the jury in applying that law to the facts before it." *United States v. Bilzerian*,

926 F.2d 1285, 1294 (2nd Cir. 1991). The government, therefore, does not seek to elicit any opinion that would invade the province of the Court or jury. For example, the government will not ask any expert to opine on whether the defendant's conduct violated IEEPA or whether ADI's technology satisfies the definition of a trade secret.

2. **Admissibility of Summary Exhibits - Fed. R. Evid. 1006**

The government will offer several summary exhibits at trial, carefully hewing to the requirement that each "fairly represent the underlying documents and be accurate and non-prejudicial." *See United States v. Milkiewicz*, 470 F.3d 390, 398 (1st Cir. 2006). Examples include summaries of (a) thousands of files the defendant downloaded from ADI's server, along with corresponding evidence of uploads to his Google Drive account; (b) thousands of files the defendant possessed that matched, by hash value, files on ADI's server; (c) the identity and number of the MMIC's Win produced for the defendant; and (d) bank records reflecting receipts and expenditures in Tricon's account.

The government will also offer summaries allowed under Rule 611(a) as "pedagogical devices to clarify and simplify complex [expert] testimony . . . ." *Id.* at 397. For example, a summary presentation is essential to the jury's understanding of how the degree to which geometric features on microchips the defendant produced match those on the corresponding ADI microchips show that they share a common source.

3. **Admissibility of Evidence of Loss Caused by Theft of Trade Secrets**

Consistent with this Court's practice of requiring that offense characteristics be proven to the jury beyond a reasonable doubt, the government will offer evidence of loss, as defined in U.S.S.G. § 2B1.1 n.3.A, caused by the defendant's theft of numerous trade secrets. This evidence will include but is not limited to the trade secrets specified in the SSI. *See* section I.F.1., *supra*.

4. Admissibility of Other Bad Acts Evidence - Fed. R. Evid. 404(b)

The government does not seek to admit Rule 404(b) evidence but will seek agreement that matters such as evidence of theft and loss beyond the four corners of the SSI and the defendant's use of pseudonyms are directly relevant to loss, motive, and consciousness of guilt.

5. Preclusion as Irrelevant of Testimony Regarding or Argument that Reverse-Engineering Is a Defense to Theft of Trade Secrets

In describing likely expert-witness testimony, the defendant indicated an intent to offer testimony that "it is not uncommon for companies that design, manufacture, and/or sell MMICs to 'reverse engineer' MMICs designed, manufactured, and/or sold by others in order to develop competing products." To the extent such evidence is offered to support an argument that the technology at issue is readily ascertainable and, thus, not a trade secret, its admission goes to an element of the offense and is likely unobjectionable. *See* 18 U.S.C. § 1839(1(3)(B). However, if the defendant were to claim that *the possibility that technology could be reengineered* is relevant to whether he obtained it by "improper means," *i.e*. stole it, such evidence would be relevant only to an affirmative defense and thus only admissible if the defendant were first to produce sufficient evidence to create a triable issue. *See* 18 U.S.C. § 1839(6)(B). "[T]o present [an] affirmative defense, a defendant must first carry the burden of production, measured by the sufficiency-of-the-evidence standard." *United States v. Cascella*, 943 F.3d 1, 6 (1st Cir. 2019).

6. Preclusion of Irrelevant Testimony and Argument, Including Testimony Aimed at Jury Nullification

Throughout the motion practice in this case, the defendant has made irrelevant and unfounded claims concerning matters that, in addition to being irrelevant, risk confusing the jury and inviting them to ignore the law. Such claims include the suggestion of ethnic bias; the availability to ADI of civil remedies; the suggestion that ADI was responsible for initiating the

investigation of the defendant's crimes;[13] and the fact that the Department of Commerce, upon further review of specific MMIC technology not charged as an illegal export in the SSI (though included in the original indictment) did not require a license. Testimony and argument on these topics are impermissible.

III. OTHER ISSUES REGARDING CONDUCT OF TRIAL

The government will also seek agreement with the defense to jointly request a Protective Order to protect trade secrets and to use chalks during opening statements.

Respectfully submitted,

NATHANIEL R. MENDELL
Acting United States Attorney

By: /s/ *John Capin*
John A. Capin
Amanda Beck
Jason A. Casey
Assistant United States Attorneys
One Courthouse Way, Suite 9200
Boston, MA 02210
(617) 748-3100
John.Capin@usdoj.gov

CERTIFICATE OF SERVICE

I, John Capin, hereby certify that this document was filed through the Electronic Court Filing system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

Date: December 15, 2021

/s/ *John Capin*
Assistant United States Attorney

[13] Any such claim would be false and would open the door to testimony about the true inception of the investigation, which would include evidence of prior bad acts arguably covered by Fed. R. Evid. 404(b).